/)

YS

(/search)

RESOURCES (/CATEGORY/RESOURCES)

Ransomware on the rise: what were the biggest cyber attacks of 2017?

Tarun Mittal (/author/tarun-mittal) posted on 5th December 2017

50 shares

(https://getpocket.com/save?ttps://yourstory.com/2017/12/cyber-attacks-omware-malware/?utm_source=getpocket&utm_medium=share)

In 2015, the global damage costs because of various ransomware attacks stood at $325 million. By the end of 2017, they are predicted to exceed $5 billion. Ransomware attacks are growing (https://blogs.cisco.com/financialservices/ransomware-lessons-for-the-financial-services-industry) at a yearly rate of 350 percent. A report (https://cybersecurityventures.com/2015-wp/wp-

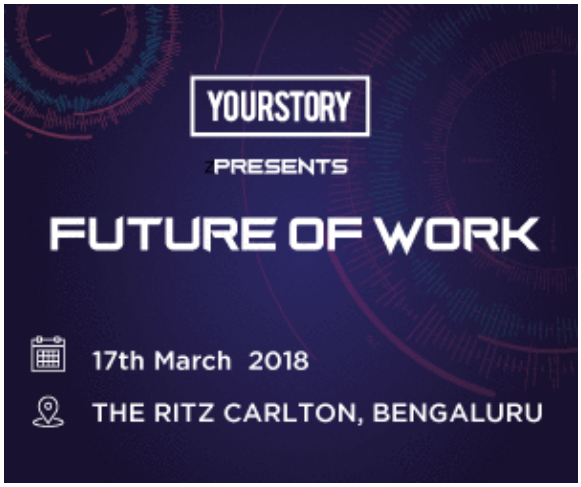
/) content/uploads/2017/10/2017-Cybercrime-Report.pdf) by Cybersecurity Ventures predicts that cybercrime will cost the world over $6 trillion annually by 2021, making it more profitable than the global trade of all major illegal drugs combined. Cybersecurity spending will correspondingly amount to $1 trillion over the next four years.

In the first half of 2017, 1.9 billion data records were either lost or stolen (https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html) through 918 cyber attacks. Most of the attacks used ransomware, a malware that infects computers and restricts access to files in exchange for a ransom. There were also several more malicious cyber attacks that destroyed data or stole millions of dollars. Among them, a few stand out for the fear they spread by exposing serious security vulnerabilities and blatant human oversight. Here are some of the worst cyber breaches of 2017:

Image: Flickr (https://www.flickr.com/photos/cyberhades/19888328041)

WannaCry

/)



WannaCry was a worldwide ransomware attack that targeted hundreds of thousands of computers in over 150 countries. The ransomware encrypted the hard drive contents of infected computers and the WannaCry perpetrators then demanded payment in Bitcoin to unlock them. WannaCry (/tag/wannacry) is considered among the worst cyber attacks of its kind not only because of its widespread impact but also the reason behind its working.

What worried the cybersecurity community the most was that the malware exploited a vulnerability in the Microsoft Windows operating system using a code which had been developed by the US National Security Agency. This code, called EternalBlue, was then stolen and leaked to the world by a group called TheShadowBrokers. Despite Microsoft having patched the zero-day vulnerability (https://en.wikipedia.org/wiki/Zero-day_(computing)) a few weeks before the WannaCry attack, several systems hadn't been updated and were thus left open to the ransomware.

NotPetya

In July 2017, a malware that at first seemed very similar (https://www.csoonline.com/article/3233210/ransomware/petya-ransomware-and-notpetya-malware-what-you-need-to-know-now.html) to a 2016 ransomware called Petya began spreading across computers around the world, with infection sites focused in and around Ukraine. But while Petya was a ransomware which demanded payment for unlocking

the encrypted hard drives of infected systems, NotPetya was something far worse. Not only was it *not* a ransomware, it encrypted all the files in an infected system, causing irreparable damage to its hard drives.

By using NSA-developed Windows vulnerabilities EternalBlue (http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch) and EternalRomance, NotPetya could spread from one computer to another without the need for human intervention (such as downloading it from a spam email, launching it, or giving it admin permissions). Due to its epicentre in Ukraine, NotPetya has been touted as a state-sponsored cyber attack orchestrated by Russia, which has been in conflict with its neighbouring country since the occupation of Crimea in 2014.

Equifax

US-based Equifax is one of the largest consumer credit reporting agencies in the world that collects and aggregates information from over 800 million individuals. In September this year, the company made a startling announcement that a massive breach of its security had compromised the information of 143 million customers. Exploiting website application vulnerabilities in a tool called Apache Struts from May to July, hackers acquired Social Security numbers, driver's license numbers, addresses, credit card numbers, and other information that can be used to perpetrate identity theft.

/) Equifax's response (https://www.bloomberg.com/news/articles/2017-09-08/consumers-struggle-to-get-answers-from-equifax-after-massive-hack) to this breach – which affected individuals in the US, Canada, and the UK – was dismal, to say the least. What's more, it was later revealed that the company *knew* about the vulnerability (https://www.usatoday.com/story/money/2017/09/14/equifax-identity-theft-hackers-apache-struts/665100001/) beforehand and failed to implement a security fix in a timely manner.

MongoDB

MongoDB is an open-source NoSQL database programme that has been the subject of several different cyber attacks this year. By exploiting a vulnerability in unsecured MongoDB installs, a group of hackers infected over 27,000 systems (https://thehackernews.com/2017/01/mongodb-database-security.html) with ransomware from the last week of December 2016 to the first week of January 2017. MongoDB promptly posted an advisory (https://www.mongodb.com/blog/post/how-to-avoid-a-malicious-attack-that-ransoms-your-data) on how users can take security measures to avoid such ransomware attacks. Despite this, September saw a resurgence of the cyber attacks, and this time 26,000 (http://www.zdnet.com/article/mongodb-ransacking-starts-again-hackers-ransom-26000-unsecured-instances/) MongoDB databases were wiped out by three groups of hackers. Just like in the first attack, the hackers demanded payment in the form of bitcoins in return for the data their victims had lost.

Elasticsearch

In January 2017, mere days after the MongoDB ransomware attacks shook the cybersecurity community, similar attacks were carried out against Elasticsearch users. Thousands of Elasticsearch servers were infected with ransomware that wiped data indices and demanded a Bitcoin payment in return for the information. Elasticsearch is a popular, open-source Lucene-based search engine library used by sites like SoundCloud, Wikipedia, and Pandora. Several users, especially those deploying it on Amazon Web Services (AWS), were unaware that Elasticsearch instances are open to cyber attacks unless certain security measures (http://code972.com/blog/2017/01/107-dont-be-ransacked-securing-

/) your-elasticsearch-cluster-properly) are taken. Had programmers been aware of this, a ransomware attack of this magnitude could never have been perpetrated.

Cloudbleed

Cloudbleed was the name of a security bug discovered in February 2017 in the reverse proxies generated by popular website performance and Security-as-a-Service provider CloudFlare. Exploiting a glitch that caused CloudFlare's servers to return extra data in response to website requests, the bug leaked sensitive data (https://techcrunch.com/2017/02/23/major-cloudflare-bug-leaked-sensitive-data-from-customers-websites/) of affected users, including passwords, authentication tokens, and more. Discovered by the team at Google's Project Zero (https://bugs.chromium.org/p/project-zero/issues/detail?id=1139), the bug leaked potentially damaging information for almost six months – from September 2016 to February 2017 – before its discovery. Major CloudFlare users such as Uber, dating platform OKCupid, and fitness programme Fitbit were affected, although the exact extent of the damage is unclear.

Zomato hack

On May 18, 2017, Indian restaurant search and delivery service, Zomato revealed that it had been the victim of a massive cyber attack. In a blog post (http://www.thehindubusinessline.com/multimedia/archive/03165/Zomat the service revealed that 17 million user records had been stolen from its database, making it the 6th largest data breach in the first half of 2017, according to a report by digital security firm Gemalto (http://indianexpress.com/article/technology/tech-news-technology/zomato-data-breach-sixth-biggest-in-first-half-of-2017-report-4854401/). User email ids and passwords were stolen by hackers; however, as Zomato stores payment-related information a separate highly secure location, no payment or credit card data was stolen. Zomato encouraged its users to promptly change their passwords; rumours also surfaced (https://www.hackread.com/zomato-hacked-17-million-

/) accounts-sold-on-dark-web/) of an online user going by the name of "nclay" claiming responsibility for the attack and selling data from the breach on a Dark Web marketplace.

HBO hack/*Game of Thrones* leaks

In perhaps one of the most high-profile cybersecurity attacks of 2017, popular television network HBO was hacked (http://www.business-standard.com/article/companies/hackers-are-coming-hbo-faces-cyber-attack-game-of-thrones-data-leaked-117080100127_1.html) in late July by a group of hackers. The group claimed to have stolen roughly 1.5 terabytes of information from the company, including scripts and episodes of popular TV show *Game of Thrones*. After initially demanding money for the return of the data, the hackers eventually posted the episodes on torrenting websites like The Pirate Bay. This attack was followed a few weeks later by another high-profile attack (https://www.cnbc.com/2017/08/17/hbo-social-media-accounts-hacked-in-another-cyberattack.html) on HBO's social media channels, with well-known group OurMine taking over the brand's Twitter and Facebook feeds for brief periods of time.

Ethereum

Cryptocurrency prices scaled new heights this year, which only made their illegal acquisition that much more tempting to certain criminals. While there were several cryptocurrency heists in 2017, the two biggest ones involve Ether, a currency on the blockchain-based app platform Ethereum.

In the first instance, a hacker targeted CoinDash's Initial Coin Offering (/2017/11/new-fundraising-craze-top-icos-2017/) in which the company was selling its own tokens in exchange for Ether. By changing the wallet address on the company's website to their own, the hacker made off with $7.4 million in the three minutes before CoinDash identified the breach and shut down the event. Even after the ICO was compromised and the news of it revealed, several investors continued to send Ether to the wallet, which took the total loss (https://www.coindesk.com/coindash-ico-hacker-nets-additional-ether-theft-tops-10-million/) in theft to around $10 million. Mere days after this, $30 million

/) (http://www.businessinsider.com/report-hackers-stole-32-million-in-ethereum-after-a-parity-breach-2017-7?IR=T) worth of ethers were stolen from users of the Parity wallet.

Apart from these major cyber breaches, 2017 also saw revelations from two big companies – Uber and Yahoo – of older devastating cyberattacks. Uber came under a lot of fire after revealing that it had deliberately covered up a massive cybersecurity breach in October 2016 (https://www.forbes.com/sites/bizcarson/2017/11/21/uber-hack-payoff-57-million-data-exposed/) that saw 57 million user records being stolen. The company covered up hushed up the entire debacle, including paying $100,000 to the hackers. In another shocking piece of news, Yahoo revealed (http://www.telegraph.co.uk/technology/2017/10/03/yahoo-says-3-billion-accounts-affected-2013-data-breach/) that every single account in its database – all 3 billion of them – had been compromised in the 2013 security breach on the platform, making it one of the largest cyber attacks in history.

Because of the evolving nature of cyber attacks, today anybody could be at risk, especially tech-based startups that rely heavily on technology that could be exploited for harm. So how do you protect your assets and avoid being the next victim of a ransomware attack? For starters, take a refresher course in cybersecurity (/2017/05/how-to-survive-a-wannacry/), and make sure your cybersecurity protocols are routinely updated. After all, one can never be too safe.

Report an Issue (/support/cyber-attacks-2017-ransomware-malware)

/)

0 Comments Sort by **Newest**

Add a comment...

Facebook Comments Plugin

Author

YS

Tarun Mittal

(/author/tarun-mittal)

Correspondent at YourStory.

(/author/tarun-mittal)

Related Topics

EQUIFAX (/TAG/EQUIFAX) MONGODB (/TAG/MONGODB) ZOMATO (/TAG/ZOMATO) HBO (/TAG/HBO)

CYBERCRIME (/TAG/CYBERCRIME) CYBERWARFARE (/TAG/CYBERWARFARE)

GAME OF THRONES (/TAG/GAME-OF-THRONES) OURMINE (/TAG/OURMINE)

MALWARE (/TAG/MALWARE) RANSOMWARE (/TAG/RANSOMWARE)

CYBERATTACK (/TAG/CYBERATTACK)

WANNACRY RANSOMWARE ATTACK (/TAG/WANNACRY-RANSOMWARE-ATTACK)

ELASTICSEARCH (/TAG/ELASTICSEARCH) CLOUDFLARE (/TAG/CLOUDFLARE)

(/trending)Trending Posts

/)

/)

What to Read Next

STARTUP (/CATEGORY/YS-STARTUP)
GovBlocks — the open protocol asking us to try decentralising governance with Blockchain (/2018/03/govblocks-blockchain-governance/)

(/2018/03/govblocks-blockchain-governance/)

/) STARTUP (/CATEGORY/YS-STARTUP)
7 startups from Bhubaneswar setting the benchmark for aspiring entrepreneurs in Odisha (/2018/03/7-startups-bhubaneswar-setting-benchmark-aspiring-entrepreneurs-odisha/)

(/2018/03/7-startups-bhubaneswar-setting-benchmark-aspiring-entrepreneurs-odisha/)

STARTUP (/CATEGORY/YS-STARTUP)
Lymbyc offers virtual assistance for companies' Big Data needs (/2018/03/lymbyc-offers-virtual-assistance-companies-big-data-needs/)


(/2018/03/lymbyc-offers-virtual-assistance-companies-big-data-needs/)

WOMEN'S EMPOWERMENT (/CATEGORY/WOMENS-EMPOWERMENT)
For over 17 years, this organisation has been lending a helping hand to underprivileged mothers (/2018/03/njmpk-underprivileged-mothers/)


(/2018/03/njmpk-underprivileged-mothers/)

STARTUP (/CATEGORY/YS-STARTUP)
Bengaluru-based Automovill takes the wheel, provides car owners access to hassle-free car service (/2018/03/bengaluru-based-automovill-takes-wheel-provides-car-owners-access-hassle-free-car-service/)

(/2018/03/bengaluru-

/)

based-automovill-takes-wheel-provides-car-owners-access-hassle-free-car-service/)

STORIES (/CATEGORY/YS-STORIES)
Foodpreneur Aditi Mammen Gupta handles two full-time jobs. Find out her secret sauce (/2018/03/posh-nosh/)

(/2018/03/posh-nosh/)

Looking for a job?

Find one on our Job Platform

See Jobs (https://yourstory.com/jobs/)

/)

Built with love in India

Report an issue (/support/)